使用联盟区块链实现安全高效的科研项目管理

孟庆峰，孙润耕

摘要

随着知识经济的发展，科学技术在社会发展中发挥着越来越重要的作用。政府和企业对科研的投入明显增加，科研项目数量也呈现出明显的上升趋势。由于缺乏规范统一的科研项目管理方案，导致不少项目逾期甚至失败，项目资金管理混乱。此外，产出成果有限，实际转化率低。本文提出了一种基于联盟区块链的科研项目管理系统。首先将科研项目管理流程规范化，然后根据这个规范，我们设计了一个符合联盟区块链、智能合约、IPFS 系统的科研项目管理系统。通过使用这些技术，我们解决了传统科研项目管理中的两大问题：违约和保密。仿真结果表明，与传统的科研项目管理相比，本文提出的方案能够显著提升项目的效率和成功率，减少项目实施过程中所消耗的时间和人力。

关键词：科研项目管理、区块链、智能合约、联盟区块链

1 介绍

由于社会经济的发展和国家政策的支持，近年来高校、科研院所、企业的科研项目数量逐渐增加。而且，涉及科研项目的领域越来越广，科研经费也在不断增加，导致项目管理过程中的人力沟通和监督成本越来越高。目前，科研项目管理的观念比较落后，缺乏科学的和规范的科研项目管理制度。此外，科研管理的信息化水平不高，容易出现以下问题：科研项目逾期甚至终止失败、科研项目资金违规使用、科研项目外泄、科研项目转化率低。因此，建立完整、科学、规范、保密的科研项目管理制度具有十分重要的意义。

一个高效的科研项目管理体系，必须具备以下特征：首先，它应该是规范的，将项目管理划分为多个流程，并严格按照流程开展科研，以防止出现延迟甚至失败的科研项目。其次，需要有一套完整的量化体系，对科研项目的各项指标和预期完成目标进行量化，从而更科学地解释项目在阶段检查和最终结果验收中是否达到预期。值得注意的是，保密性也非常重要。根据《国家保密局秘密科研项目管理条例》，项目单位必须有健全的保密制度和组织，防止科研项目泄露等现象的发生。

目前，主流的项目管理方法有项目管理学会发布的《项目管理知识体系》(PMBOK)、英国商务部(OGC)的《受控环境中的项目(PRINCE2)》[19]、《全球项目管理方法论》(WW- PMM)[16]。这些方法试图使项目团队的活动标准化，从而使预测、管理和跟踪更容易。

本文提出了一种基于联盟区块链的科研项目管理系统，旨在规范科研项目管理，减少科研项目管理中出现的一系列问题。在该系统中，提出了对科研项目各项指标进行量化的方案，可以更方便、直观地查看项目进展情况。结合联盟区块链和智能合约的特点，我们认为该系统可以最大程度地节省传统科研项目管理的人力和时间成本。同时，采用星际文件系统(InterPlanetary File System, IPFS)对科研项目产生的文件进行管理，在降低成本的同时保证了数据的安全。

本文的主要贡献如下：

1. 结合现有项目管理流程体系，提出了科研项目指标量化方案，并给出了项目完成系数的近似算法。
2. 设计了符合联盟区块链和 IPFS 的科研项目管理系统，利用智能合约规范科研项目管理流程，利用 IPFS 系统解决科研项目管理中的数据存储和隐私保护问题。
3. 在做了一个实验来测试系统的时间消耗后，我们得到的结果是时间消耗只与请求次数相关，而与文件大小无关。

论文的其余部分组织如下。第 2 节主要介绍现阶段国内外的相关研究工作。第 3 节介绍了相关背景知识，包括科研项目管理、区块链、智能合约和 IPFS。此外，我们定义了问题；在第 4 节介绍了系统模型和设计目标。第 5 节详细介绍了按照联盟区块链设计的科研项目管理系统。在第 6 节中，我们使用仿真实验来验证我们系统的性能。最后，我们在第 7 节总结了我们的论文。

2 相关工作

目前，在国际上有两种广为人知的项目管理研究体系：国际项目管理协会(IPMA)和美国项目管理学会(PMI)[8, 27, 35, 36]。1996 年，PMI 发布了项目管理知识体系(PMBOK)，并于 2017 年更新到第六版。此外，中国的中国项目管理知识体系(C-PMBOK)已经更新到第二版，内容得到了扩展和加强。

基于对现有项目管理文献和其他成功学科的回顾和分析，Frederik Ahlemann

等人开发了一个框架，为基于理论的规定性项目管理提供指导，这可能有助于建立可行的规定性研究设计[1]。

Farzana Asad Mir 等人利用阿联酋项目组织中项目管理专业人员的经验，研究了项目管理绩效与项目的成功之间的关系。研究表明，项目管理绩效与项目的成功存在一定的关系，组织可以通过更加重视这种关系[21]来提高项目的成功率。此外，区块链以其不可驯服、匿名、去中心化、无信任等独特特性，在许多应用领域大放异彩。国内外很多基于区块链的应用覆盖了金融行业、安全问题、物联网(IoT)、能源等诸多领域[10, 13, 25, 28, 32]。

在麻省理工学院，学生可以使用区块链技术来管理自己的学习记录，他们只需要下载一个名为 Blockcerts Wallet 的 APP。在这个 APP 中，学生不仅可以查看毕业证，还可以看到学分、专业证书和成绩单。在发布区块链数量的学术证书 block certs 开放标准[12,17]之前，该 APP 源自 MIT 媒体实验室，该标准由颁发者、证书、验证者和钱包四个组件组成。

Al-bassam, Mustafa 基于区块链设计了一个名为 SCPKI 的系统，以取代传统的公钥基础设施 (PKI)系统[20]。由于其透明和去中心化的设计，该系统可以通过使用以太坊上的智能合约轻松验证证书是否为盗版。由此可见，这个去中心化设计的系统可以有效防止证书颁发机构向目标发放伪造证书。

区块链与隐私保护结合后，孟深等人将其应用于医疗数据保护、物联网等领域[9, 14, 18, 29, 30, 34]。

3 背景

3.1 科研项目管理

项目管理起源于美国，其中以关键路径法(CPM)和项目评估与评审技术(PERT)为代表。随着时间的推移，出现了越来越多的标准化项目管理方法，例如 PMBOK、PRICNCE2 和 WWPMM。

3.1.1 PMBOK

根据美国项目管理学会(PMI)提出的项目管理知识体系(PM-BOK)，项目管理分为五个主要过程和十个知识领域。这十大知识领域分别是：项目集成管理、项目范围管理、项目时间管理、项目成本管理、项目质量管理、项目人力资源管理、

项目沟通管理、项目风险管理、项目采购管理、项目利益相关者管理。

3.1.2 PRINCE2

PRINCE2 是受控环境项目(Project IN Controlled Environment)的缩写。隶属于政府商务办公室(OGC)，于 1996 年引入，是一个结构化的项目管理流程。主要流程如下：指导项目(DP)、启动项目(SU)、引入项目(IP)、控制阶段(CS)、管理产品交付(MP)、管理阶段边界(SB)、关闭项目(CP)[15]。

虽然使用的术语不同，但 PMBOK 和 PRINCE2 是高度兼容和互补的。将这两个项目管理标准结合起来，可以为我们的项目管理提供更有效的方法。我们将项目管理流程概括为：项目启动、项目申报、项目执行、阶段控制、项目收尾。此外，还涉及到项目时间管理、项目成本管理和项目质量管理。

3.2 区块链和智能合约

3.2.1 区块链

区块链是一个全局维护和共享的分布式分类账，或者是一个仅可添加和查看的分布式全局数据库[6]。交易一旦写入数据库，就不能删除或修改。区块链包括去中心化、不信任、数据共享、匿名和非干扰等特性。

区块链技术起源于比特币。2008 年 11 月，一个自称“中本聪”的人发表了文章《比特币：对等电子现金系统》[22]，阐述了如何在没有信任体系的情况下建立一个去中心化的点对点交易系统。从此，区块链进入了公众的视野。截至 7 月 30 日，比特币的总市值已达到 1690 亿美元，占所有数字加密货币总市值的 64%以上。虽然密码学本身争议很大，但底层的区块链技术非常有价值，因此目前被广泛应用于多个领域[24]。

根据访问机制的不同，区块链可以分为三类：公有区块链、联盟区块链和私有区块链。在表 1 中，我们对这三种区块链进行了详细的比较[32, 33]。

从三种不同的区块链的特点可以看出，联盟区块链非常适合两家或数量有限的机构参与科研项目的活动，联盟区块链的访问机制和去中心化可以在很大程度上增加科研项目过程中的机密性。

表 1 三种区块链的比较

财产	公有区块链	联盟区块链	私有区块链
参与者	所有矿工	指定的机构	个人的或组织内部
激励机制	需要	可选	不需要
中心化程度	分散	多个中心	集中
速度	慢	快	快
使用场景	加密数字货币	组织间的业务合作	内部管理

3.2.2 智能合约

实际上，智能合约的概念早于区块链，区块链最早是由计算机科学家和密码学家 Nick Szabo 在 1994 年提出的[5]。它被描述为一系列以数字方式指定的承诺，包括各方要履行的协议。直到 2008 年区块链的概念被提出，智能合约才有可能发挥作用。然而，随着以太坊的诞生，智能合约在 2013 年首次得到广泛认可。在以太坊白皮书中，智能合约被描述为“涉及由一段实现管理规则的代码直接控制数字资产的复杂应用程序”[20]。

从技术上讲，智能合约是一种计算机程序，它在发布到区块链之前设定所有的程序，并为用户提供一个使用该程序的接口。一旦程序发布到链上，就无法更改。相反，它将始终自动运行，并生成相应的数据。

智能合约具有以下优点：(1)执行准确，(2)人为干预风险低，(3)去中心化，(4)运行成本低[7, 11, 23, 31]。由于智能合约的性质，存在着很多风险：由于智能合约一旦发布就无法更改，如果一开始在设计上有漏洞，将会造成无法挽回的损失。2016 年 5 月，以太坊历史上最大的众筹项目 TheDAO 完成了 1.5 亿美元的众筹项目。然而，仅仅一个月后，它就遭到黑客攻击，损失了价值 6000 万美元的 ETH。因此，我们需要充分利用智能合约的优势，同时避免可能的风险。

3.3 IPFS

像以太坊这样一个完整的智能合约系统，可以被理解为一个可编程的分布式数据库，由于其消耗 Gas 的机制，无法在以太坊上存储大量数据。IPFS 是一种点对点数据分发协议，其节点形成分布式文件系统[2-4]。IPFS 可以看作是一个比特流群，在一个 Git 库中交换对象。此外，它为每个文件生成一个唯一的哈希值，

构建哈希值到文件的映射。当对文件进行查询时，查询的基础可以是哈希值。此外，IPFS 在便捷性、安全性和开放性等方面具有许多优势。IPFS 和区块链的结合为分散存储不断增长的数据提供了一种可行的替代方案。

4 问题定义

本文提出了一种基于联盟链的科研项目管理系统，该系统与智能合约自动运行在联盟链上，使用 IPFS 系统保存加密文件。本节定义了围绕系统模型和设计目标的问题。

4.1 系统模型

该系统围绕运行在联盟区块链上的智能合约和 IPFS 系统建立相应的系统。如图 1 所示，系统中的实体分为三类：参与项目的机构、IPFS 系统和联盟区块链平台。这三类主体围绕联合体区块链平台实现高效的科研项目管理。

4.1.1 参与项目的组织和机构

项目参与主体主要覆盖政府、高校、企业、科研院所等组织或机构。在这个系统中，他们以区块链节点的身份加入联盟区块链。

4.1.2 IPFS 系统

由于 Gas 机制对运行在以太坊联盟链上的智能合约的限制，无法存储大量的数据文件，但在科研项目的进行过程中会产生大量的文件，使用 IPFS 可以确保数据文件的存在并加强其保密性。

4.1.3 联盟区块链平台

联盟区块链更符合项目参与方对隐私保护、项目信息保护、高效运营的要求。除了项目的某些初始属性外，IPFS 系统中项目所需文件的一些项目进度指标、时间节点和哈希值也存储在区块链上。

4.2 设计目标

本系统是基于联盟区块链和 IPFS 系统的科研项目管理系统，主要目标有三个：

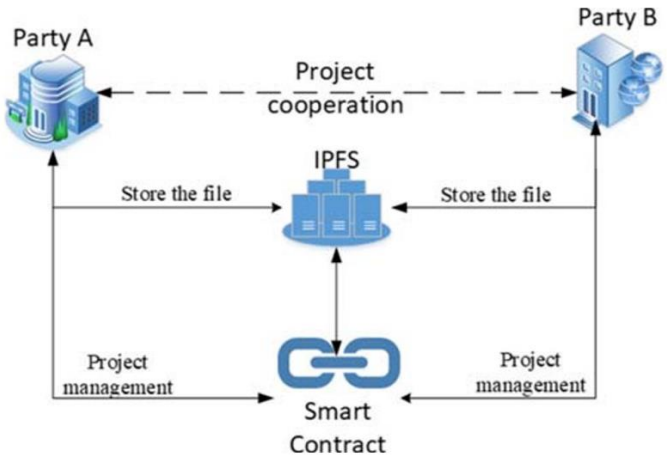

图 1 系统实体模型

1. 安全性：由于大多数科研项目涉及国家或企业的机密信息，必须保证管理系统的安全性。
2. 效率：尽量减少参与科研项目管理的人员，专注于科研。
3. 合规性：防止项目因一个参与者违约而终止或失败。

为了实现这三个目标，我们主要采用区块链和 IPFS 联盟。一旦执行无法终止，由于智能合约的性质，项目中的所有操作都将被记录在链块上。而且，它不能被篡改和删除，保证了项目的执行，防止了一方违约。同时，可以降低参与项目管理的人力。在安全问题上，联盟链首先需要授权一定程度的访问机制，这样才能保障数据的安全。对于深度加密过程中创建的项目文件，我们将 IPFS 与非对称加密系统相结合，以保证数据安全，最大限度地防止数据泄露。

5 研究基于联盟区块链的项目管理系统

5.1 系统概述

本系统的根本目的是实现从项目启动到项目结束的全过程管理，该系统的实现主要采用基于联盟链的智能合约技术和 IPFS 系统结合非对称加密技术。

有权访问该系统的人必须是授权的组织或机构，可以作为区块链节点加入联盟区块链。授予人可在系统内发起或申报他人发起的项目，建立合作关系后再启动科研合作。在合作过程中，所有资金转账、进度检查提示等工作，都将由智能合约自动执行。

5.2 系统模块组成

本系统主要由两个功能模块组成：数据文件加密模块和联盟链模块。

5.2.1 数据文件加密模块

文件加密模块主要利用星际文件系统(IPFS)和非对称密码技术。如图 2 所示，当 A 想要通过区块链将文件发送给 B 时，A 首先获取 B 的公钥，然后用它对文件进行加密。然后，A 使用 IPFS 将加密后的文件添加到 IPFS 中，获取文件的哈希值。该哈希值通过区块链发送给 B 后，B 会接收到该哈希值，并通过 IPFS 获取该文件。然后，用 B 自己的私钥对哈希值进行解密，获得完整的文件。

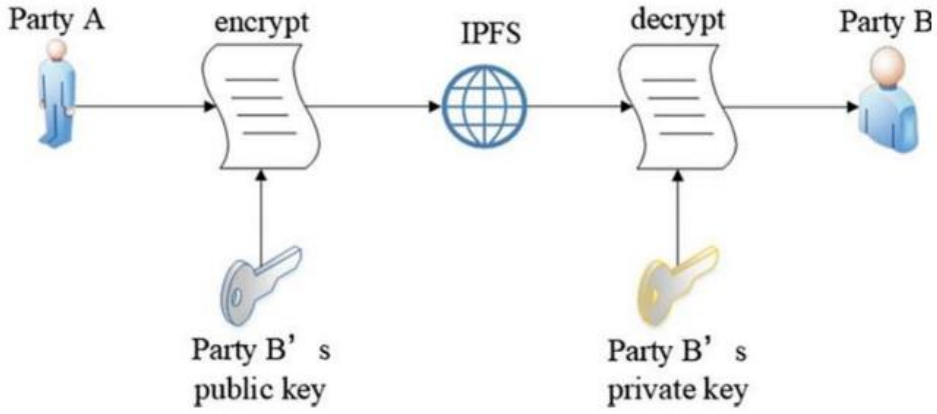

图 2 加密模块示意图

5.2.2 联盟区块链模块

项目参与方之间的互动，通过联盟链模块进行。如图 3 所示，区块链共享账号是由按时间顺序链接在一起的区块组成的。每个区块包含若干个交易，其中以指定格式存储项目的所有数据。存储数据的格式如表 2 所示；

项目数据存储了当前项目的所有数据，包括甲乙双方地址、项目基本信息、项目时间节点数组、项目进度指标数组、项目中的数据文件等。

- 时间节点：包含时间节点的名称、时间、描述信息
- 进度指标:包含名称、值、类型和描述
- 数据:包含名称、来源、公钥、哈希值和描述

联盟区块链模型负责系统运行和项目参与者之间的数据交互。智能合约部署在区块链上后将自动执行。值得注意的是，合约不能再变化，可以有效防止项目参与者违约。

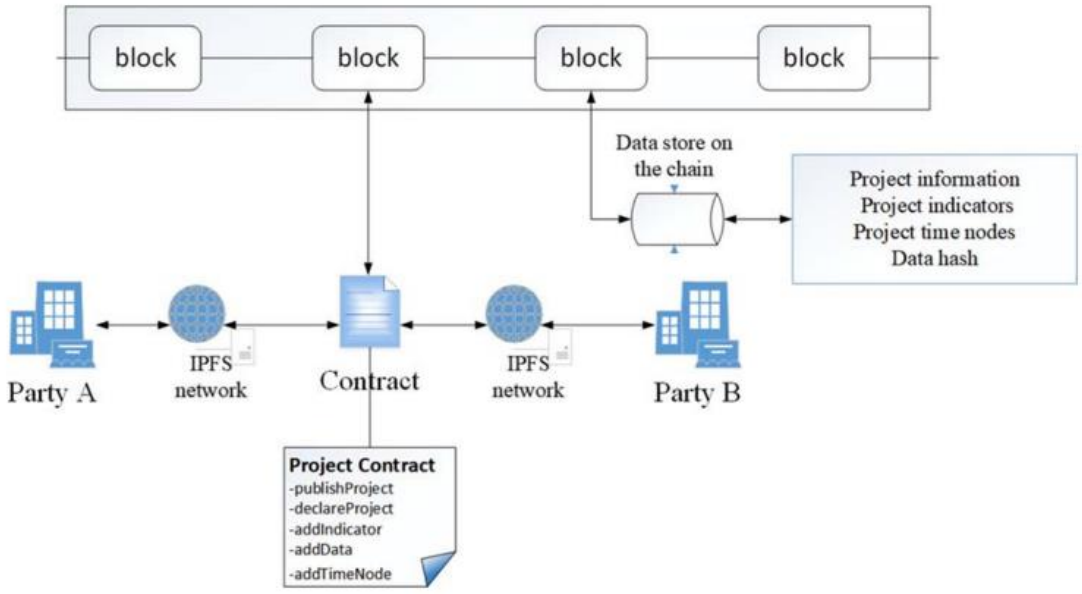

图 3 联盟区块链模块示意图

表 2 智能合约上的项目数据结构

属性名	类型	描述
Name	string	项目名称
partyA	address	甲方地址，甲方余额可从中获取
partyB	address	乙方地址，乙方余额可从中获取
startTime	uint	项目开始时间
endTime	uint	项目结束时间
totalFund	uint	项目总资金
startFund	uint	启动项目资金
timeNodes	TimeNode[]	项目的一些时间节点
Indicators	Indicator[]	项目部分进度指标
Datas	Data[]	项目的数据

5.3 系统工作流程

系统工作流程序列图如图 4 所示：

1. 项目启动前，甲方将 IPFS 系统上的项目邀请函及其公钥直接上传至联盟链，供所有授权机构核查。
2. 当 C 组织或机构有意与甲方合作时，将使用甲方的公钥加密将完成的项目申报或其他材料上传到 IPFS 系统。在获得数据的哈希值后，再将哈希值和

C 组织或机构的地址与区块链一起写入联盟区块链上，并发送给甲方。

3. 甲方在收到项目申报单等加密文件的哈希值后，首先通过 IPFS 系统获取加密的项目申报单等资料。然后，甲方使用自己的私钥进行解密，获得真实的文件。根据项目申报，将对审计申报进行讨论。如甲方同意与 C 组织合作开展科研项目，则需要用算法 1 初始化部分项目属性，包括:甲方、乙方地址、项目启动时间、项目结束时间、项目总资金、启动资金、一些排序时间节点（用于成果检验）、以及一些自定义项目指标。然后，甲方需要将科研经费总额转入合同，并使用乙方公钥对项目合同进行加密，上传到 IPFS 系统，并将哈希值传递给链。当甲方初始化完成后，乙方将收到项目的初始化信息。

Algorithm 1 initializeProject.

Input: startTime, endTime, totalFund, startFund, TimeNodes[], Indicators[]
Output: Transfer project information to the chain

```
1: project.startTime ← startTime;
2: project.endTime ← endTime;
3: project.totalFund ← totalFund;
4: project.startFund ← startFund;
5: project.partyA.balance ←
   project.partyA.balance − project.totalFund
6: project.balance ← project.totalFund
7: for i = 0 to m do
8:     project.timeNodes.push(TimeNodes[i]);
9: end for
10: for i = 0 to n do
11:     project.indicators.push(Indicators[i]);
12: end for
```

4. 当乙方同意项目信息正确时，项目启动，智能合约自动将指定的启动资金转账至乙方地址。

5. 当到达时间节点时，合同将向乙方发送请求，此时，乙方将按照指定的索引样式将当前阶段的结果发送到区块链。本合同通过算法 2 计算乙方目前完成的项目进度，算法 2 输入为“项目”和“指标”，其中“项目”指当前项目

的进度，“指标”指设定的项目指标。计算结果将通过合同发送给甲、乙双方。

Algorithm 2 checkSchedule.

```
Input: Project, Indicators[]
Output: result
 1: i ← 0;
 2: result ← true;
 3: while i ← indicators.length do
 4:     indicator ← indicators[i];
 5:     if indicator.type == 0 then
 6:         if indicator.value > project.indicators[i].value then
 7:             result ← false;
 8:             BREAK;
 9:         end if
10:     else
11:         if indicator.value > project.indicators[i].value then
12:             result ← false;
13:             BREAK;
14:         end if
15:     end if
16:     i++;
17: end while
18: return result, indicators[];
```

6. 在达到最终结论时间节点后，乙方使用甲方公钥对结论报告等资料进行加密并上传到 IPFS 系统。获得的哈希值应与乙方当前的进度一起发送到链中。在合同中计算出乙方的完成情况后，将完成结果与加密材料的哈希值一起发送给甲方。如未达到预期情况，甲方可根据实际情况调整工期等待乙方完成，或宣布项目失败，如有，剩余资金将转回甲方地址。如乙方达到预期目标，甲方确认项目完成。
7. 当项目相关数据和日志通过智能合约发送给甲乙双方时，项目结束。

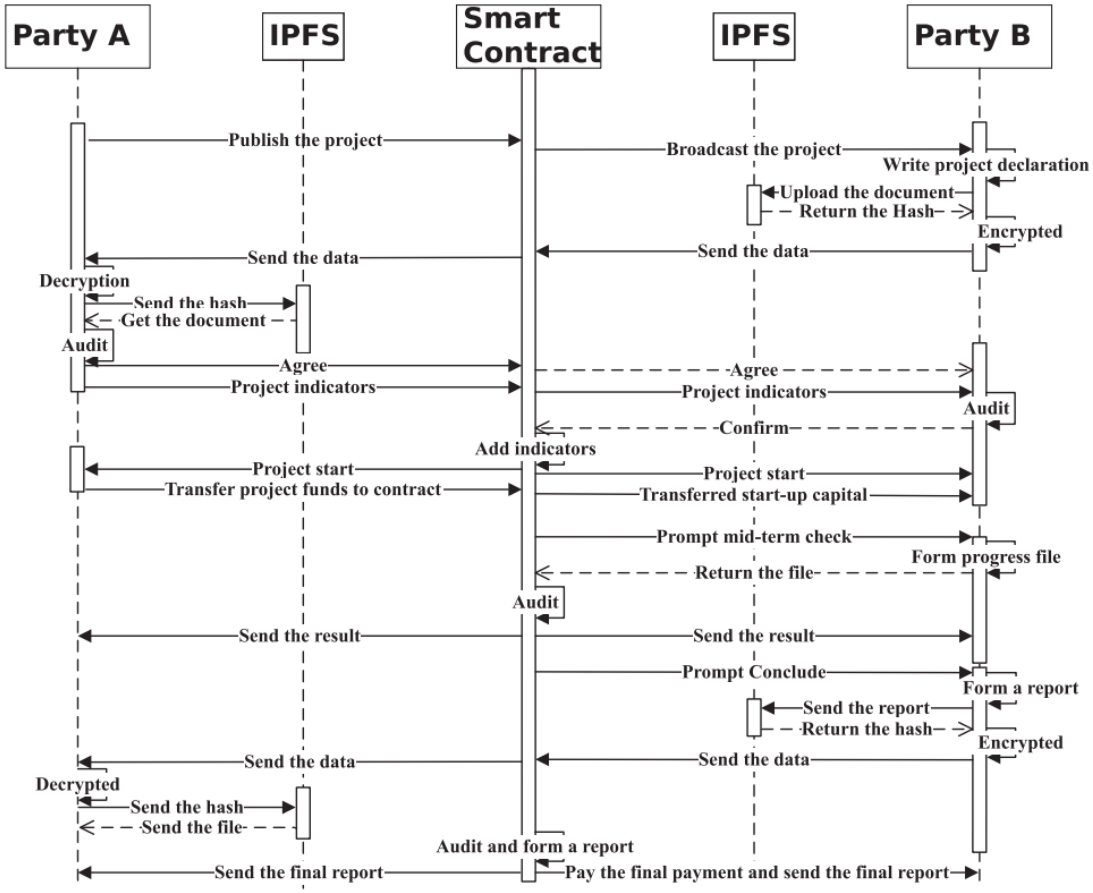

图 4 系统序列图

6 绩效评估

联盟区块链、IPFS 和非对称加密相结合，充分保障了系统的安全性。用 solemotion 语言编写智能合约，实现了从项目申报到项目结束的全过程管理。随着智能合约被部署到以太坊联盟链平台，每个组织或机构对应一个联盟链节点，可以通过控制台调用智能合约。

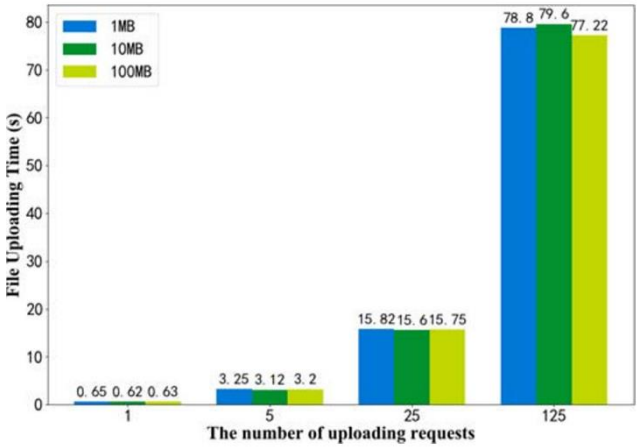

图 5 响应时间图

我们使用 PC 机模拟一个参与项目的组织，并测试其对系统请求的响应时间。请求次数分别为 1 次、5 次、25 次和 125 次。每次请求涉及的文件数据大小分别为 1 MB、10 MB 和 100 MB。代表项目参与者的 PC 配置为：Intel(R) Core(TM) i5-8300h CPU @2.30ghz 2.30ghz, 8GB RAM 和 64 位 windows 操作系统。

在我们的实验中，我们重点评估了文件上传时间，因为它是项目管理系统的一个重要性能指标。不同上传请求以及文件大小下的文件上传时间如图 5 所示。我们可以看到，即使是 100MB 的文件，上传时间也可以在 0.6s 左右，满足了实际应用的需要。我们还观察到，文件上传时间与文件大小几乎无关。这是因为 IPFS 网络返回的哈希值不大。影响上传时间的主要因素是上传请求的数量，即文件上传时间与文件数量成正比。例如，对于一个 10MB 的文件，请求 1 次、5 次、25 次、125 次的上传时间分别为 0.62s、3.12s、15.63s、79.6s。

与传统科研项目管理中手工传输文件的方式相比，该系统在保证其安全性的前提下，大大节省了人力、物力和时间。

7 结论

本文的目的是实现一个高效的科研项目管理系统。该系统利用智能合约自动执行和默认的防篡改联盟区块链数据，以及分布式全局文件数据库 IPFS 的特点，实现了一个可行的科研项目管理系统。通过仿真测试，该系统可以规范科研项目管理流程，有效减少科研项目管理和人力资本的时间，加强其私密性，提高科研项目的成功率。

在未来的工作中，我们计划对我们的系统进行增强，并进行更详细的实验来验证我们系统的安全性和安全性[26, 37]。

参考文献

1. Ahlemann, F., Arbi, F.E., Kaiser, M.G., Heck, A. (2013). A process framework for theoretically grounded pre-scriptive research in the project management field. International Journal of Project Management, 31(1), 43–56. https://doi.org/10.1016/j.ijproman.2012.03.008. The International Network for Business and Management Journals (INBAM) 2012.
2. Ali, M.S., Dolui, K., Antonelli, F. (2017). Iot data privacy via blockchains and ipfs. In Proceedings of the seventh international conference on the internet of things (p. 14): ACM.
3. Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. arXiv:1407.3561.
4. Brito, I.P., Tropaldi, L., Carbonari, C.A., Velini, E.D. (2018). Hormetic effects of glyphosate on plants. Pest Management Science, 74(5), 1064–1070.

5. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292–2303.
6. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., et al. (2016). Blockchain technology: beyond bitcoin. Applied Innovation, 2(6-10), 71.
7. Dai, P., Mahi, N., Earls, J., Norta, A.(2017). Smart-contract value-transfer protocols on a distributed mobile application platform. https://qtum.org/uploads/files/cf6d69348ca50dd985b60425ccf282f3.pdf p.10.
8. Eberle, A., Meyer, H., Rosen, D. (2011). A comparison of pmi and ipma approaches. Analysis to support the project management standard and certification system selection.
9. Gao, F., Zhu, L., Shen, M., Sharif, K., Wan, Z., Ren, K. (2018). A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. IEEE Network, 32 (6), 184–192.
10. Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking indus try. Financial Innovation, 2(1), 24.
11. Hahn, A., Singh, R., Liu, C.C., Chen, S. (2017). Smart contract□based campus demon stration of decentralized transactive energy auctions. In 2017 IEEE Power & energy so ciety innovative smart grid technologies conference (ISGT) (pp. 1–5): IEEE.
12. Hope, J. (2018). Issue secure digital credentials using technology behind bitcoin. The Successful Registrar, 17(11), 1–4.
13. Hukkinen, T., Mattila, J., Ilomaki, J., Sepp ¨ al¨ a, T., et al. (2017). A ¨ blockchain a pplication in energy. ETLA Reports, 71.
14. Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., Yu, N. (2019). Healthchain: a bl ockchain-based privacy preserving scheme for large-scale health data. IEEE Internet of Things Journal, 6(5), 8770–8781.
15. Jamali, G., & Oveisi, M. (2016). A study on project management based on pmbok an d prince2. Modern Applied Science, 10(6), 142–146.
16. Jessup, C.B., Moore, S.C., Palozzi, G., Stefanski, P.A., Trisko, S.D., Wilkie, L.E. (201 0). Method, system and program product for assessing a product development project employing a computer-implemented evaluation tool. US Patent 7,680,682.
17. Jirgensons, M., & Kapenieks, J. (2018). Blockchain and the future of digital learning credential assessment and management. Journal of Teacher Education for Sustainability, 20(1), 145–156.
18. Shen, M., Ma, B., Zhu, L., Mijumbi, R., Du, X., Hu, J. (2017). Cloud-based approxi mate constrained shortest distance queries over encrypted graphs with privacy protectio n. IEEE Transactions on Information Forensics and Security, 13(4), 940–953.
19. Matos, S., & Lopes, E. (2013). Prince2 or pmbok–a question of choice. Procedia Tech nology, 9, 787–794.
20. McCorry, P., Shahandashti, S.F., Hao, F. (2017). A smart contract for boardroom votin g with maximum voter privacy. In International conference on financial cryptography a nd data security (pp. 357–375): Springer.
21. Mir, F.A., & Pinnington, A.H. (2014). Exploring the value of project management: lin king project management performance and project success. International Journal of Proj ect Management, 32(2), 202–217.
22. Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. http://www.bitcoin.

org/bitcoin.pdf. (cited on pp. 15 and 87) (2017).
23. Savelyev, A. (2017). Contract law 2.0:‘smart’contracts as the beginning of the end of classic contract law. Information & Communications Technology Law, 26(2), 116–134.
24. Shen, M., Deng, Y., Zhu, L., Du, X., Guizani, N. (2019). Privacy□preserving image r etrieval for medical iot systems: a blockchain□based approach. IEEE Network, 33(5), 27–33.
25. Shen, M., Tang, X., Zhu, L., Du, X., Guizani, M. (2019). Privacy□preserving support vector machine training over blockchain-based encrypted iot data in smart cities. IEEE Internet of Things Journal.
26. Shen, M., Zhang, J., Zhu, L., Xu, K., Tang, X., Liu, H. (2019). Security svm training over vertically-partitioned datasets using consortium blockchain for vehicular social net works. IEEE Transactions on Vehicular Technology, 1–10.
27. Toljaga-Nikolic, D., Obradovi ´ c, V., Mihi ´ c, M. (2011). Certifica- ´ tion of project managers based on ipma and pmi models through conforming to iso 17024: 2003 1. Management (1820-0222) (59).
28. Turk, Z., & Klinc, R. (2017). Potentials of blockchain technology ˇ for construction m anagement. Procedia Engineering, 196, 638–645.
29. Guan, Z., Zhang, Y., Zhu, L., Wu, L., Yu, S. (2019). Effect: An efficient flexible priv acy-preserving data aggregation scheme with authentication in smart grid. Science Chin a Information Sciences, 62(3), 32103.
30. Guan, Z., Liu, X., Wu, L., Wu, J., Xu, R., Zhang, J., Li, Y. (2020). Cross-lingual mu lti-keyword rank search with semantic extension over encrypted data. Information Scien ces, 514, 523–540.
31. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., Wan, J. (2018). Smart contract-based acc ess control for the internet of things. IEEE Internet of Things Journal, 6(2), 1594–160 5.
32. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2017). An overview of blockchain t echnology: architecture, consensus, and future trends. In 2017 IEEE International congr ess on big data (BigData congress) (pp. 557–564): IEEE.
33. Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H. (2018). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services, 14(4), 352–37 5.
34. Zhu, L., Tang, X., Shen, M., Du, X., Guizani, M. (2018). Privacy□preserving ddos att ack detection using cross-domain traffic in software defined networks. IEEE Journal on Selected Areas in Communications, 36(3), 628–643.
35. Qiu, M., Sha, E.H.-M., Liu, M., Lin, M., Hua, S., Yang, L.T. (2008). Energy minimiz ation with loop fusion and multi□functional-unit scheduling for multidimensional dsp. Journal of Parallel and Distributed Computing, 68(4), 443–455.
36. Li, J., Ming, Z., Qiu, M., Quan, G., Qin, X., Chen, T. (2011). Resource allocation rob ustness in multi-core embedded systems with inaccurate information. Journal of System s Architecture, 57(9), 840–849.
37. Shao, Z., Xue, C., Zhuge, Q., Qiu, M., Xiao, B., Sha, E.H.-M. (2006). Security protec tion and checking for embedded system integration against buffer overflow attacks via hardware/software. IEEE Transactions on Computers, 55(4), 443–453.